Docket No. SHAI-11

REMARKS

The Examiner is thanked for his/her careful and very thorough Office Action. The Examiner is particularly thanked for the helpful suggestions regarding correction of the alleged informalities.

Claim 1 is amended. Claims 2-9 are cancelled. Claim 10 is amended to correct an informality. Claims 13 and 14 are amended to correct an informality. Claim 15 is amended. New claim 16 is added. These changes are not believed to add new matter, and their entry is respectfully requested.

The foregoing amendment to the specification is submitted to remove a typographical as pointed out by the Examiner. This change is respectfully asserted not to introduce new matter, and entry is respectfully requested.

Claim Objections

Examiner objects to claims 2, 3, 10, and 15. Claims 2-3 are cancelled. Claim 10 is amended to correct informalities as pointed out by Examiner. Claim 15 is cancelled. Therefore, these objections are believed fully addressed.

Claims 2-9 are also objected to, and, as stated above, these claims have been cancelled.

Claim Rejections under 35 USC 112 second paragraph

The various rejections under 35 USC 112, second paragraph, have been addressed by the amendments to claims 1, 10, 13 and 14. Claim 15 is cancelled. These amendments are believed to overcome the 112 rejection by correcting the informalities pointed out by Examiner. Favorable reconsideration of the claims is respectfully requested.

Claim Rejections under 35 USC 101

Claims 1-15 were rejected under 35 USC 101 as inoperable. Applicant submits the foregoing amendments, limiting the number of ciphers to two (in

Amendment – Serial No. 09/847,503...Page 10

Docket No. SHAI-11

other words, in the claim language, r=2), which addresses the inoperability, as discussed below.

According to the Blind Key Encryption algorithm described in the present application, Applicant generates two ciphers M_1 and M_2 as follows:

$M_1 = M^{e1+t} \bmod n.$

$M_2 = M^{e2+t} \bmod n.$

From the above two ciphers, one may calculate a value M_{12} as follows:

$M_{12} = [M_1.(M_2)^{-1}] \bmod n$

So the value of $M_{12} = [M^{e1+t}(M^{e2+t})^{-1}] \bmod n.$

Therefore, $M_{12} = [M^{e1+t}.M^{-e2-t}] \bmod n.$

Since the base is the same, adding the exponents in the above equation,

$M_{12} = [M^{e1+t-e2-t}] \bmod n. = [M^{e1-e2}] \bmod n.$ \hspace{1cm} (t disappears since t-t = 0)

Now, M_{12} is a cipher with a definitely known exponent, e_1-e_2.

This is how an attacker can eliminate the random number, t, from the ciphers. Now, he can compute the multiplicative inverse of e_1-e_2 which would serve as the private key (decryption key). In other words, the attacker needs to compute a value d_{12} such that

$(e_1-e_2). d_{12} = k.\phi +1.$ where k could be any integer. This can be done by running Euclid's algorithm. However, in order to be able to do this, the attacker needs ϕ, which is never known. This is because ϕ, the Euler Totient function, is discarded immediately after the keys are generated. No record is maintained of it by the key owner. When the key owner himself has no idea of it, there is no way that the attacker can make out its value. ϕ can be known, if the key modulus, n, can be factored into p and q. But this requires astronomical computation effort over which the conventional RSA algorithm is based.

Amendment – Serial No. 09/847,503..*Page 11*

PAGE 18/22 * RCVD AT 3/17/2006 3:12:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:972 980 5841 * DURATION (mm-ss):08-44

There is another approach to computing d_{12} mentioned in the above paragraph. That is bribing some one at the key owner's location and getting the private key of my Blind Key Encryption system (d_1, d_2) revealed. Recall one of my key generation equations

$d_1+d_2 = k_2 \phi$. So from the revealed key, though ϕ cannot be known, a multiple times ϕ, that is, $k_2 \phi$ can be known. Please note that ϕ and $k_2 \phi$ behave alike. In multiplicative inverse calculations ϕ acts like a slimily of zero in normal mathematical calculations.

What Euclid's algorithm does for us is given two known values e and ϕ, it will give the two values d and k satisfying the relation $e.d = k\phi+1$. Out of these two values that Euclid's algorithm returns, what is important and useful is the d value which is used as the counterpart key (private key). The other value k has no significance. So the attacker will input the values (e_1-e_2) and $k_2.\phi$. Consequently, Euclid' algorithm will return him d_{12} satisfying the relation $(e_1-e_2).d_{12} = k (k_2.\phi) +1$. This is again fine and acceptable because in place of k, now the attacker has $k.k_2$. Any multiple of ϕ is acceptable.

Finally, the extract of the whole above discussion is that the attacker needs the private key even after capturing both ciphers. This defeats Moore's attack, which teaches that the original message can be recovered without private key when both ciphers are available.

Now, we discuss the case with many ciphers. Assume M_1, M_2 and M_3 be three ciphers computed as follows:

$M_1 = M^{e1+t} \bmod n$.

$M_2 = M^{e2+t} \bmod n$.

$M_3 = M^{e3+t} \bmod n$.

Amendment – Serial No. 09/847,503..*Page 12*

PAGE 19/22 * RCVD AT 3/17/2006 3:12:04 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/6 * DNIS:2738300 * CSID:972 980 5841 * DURATION (mm-ss):08-44

Compute M_{12} and M_{23} as follows:

$M_{12} = [M_1.(M_2)^{-1}] \bmod n = [M^{e1-e2}] \bmod n$

$M_{23} = [M_2.(M_3)^{-1}] \bmod n = [M^{e2-e3}] \bmod n.$

Now, the attacker has two ciphers encrypted by two definitely know exponents e_1-e_2 and e_2-e_3. This is sufficient for the Moore's attack since what Moore teaches is that when two ciphers are available encrypted by two definitely known exponents, original message can be recovered by finding two integers r and s such that

$$r(e_1-e_2) + s(e_2-e_3) = 1.$$

Since e_1, e_2 and e_3 are known to the public as public key exponents, (e_1-e_2) and (e_2-e_3) can be calculated easily. Consequently, r and s satisfying the above Moore's relation can be computed. Finally, the attacker can compute the original message M as follows:

$M = M_{12}{}^r M_{23}{}^s \bmod n = [(M^{e1-e2})^r (M^{e2-e3})^s] \bmod n = M^{r(e1-e2) + s(e2-e3)} \bmod n$

$= M^1 \bmod n = M.$

In the previous case where we have only two ciphers, we are saved from this attack because when t is eliminated, the ciphers will reduce to one. With the single exponent, (e_1-e_2), one can not find r such that

$$r.(e_1-e_2) = 1.$$

This is not possible.

By the above arguments and the present amendments limiting the number of ciphers to two, Applicant respectfully submits that Examiner's rejection of the claims is now moot. Favorable reconsideration of the claims is respectfully requested.

Docket No. SHAI-11

Conclusion

Thus, all grounds of rejection and/or objection are traversed or accommodated, and favorable reconsideration and allowance are respectfully requested. <u>The Examiner is requested to telephone the undersigned attorney or Robert Groover for an interview to resolve any remaining issues.</u>

March 17, 2006   Respectfully submitted,

Patrick C. R. Holmes, Reg. No. 46,380
Attorney for Applicant

Customer Number 29106
Groover & Holmes
PO Box 802889
Dallas, TX 75380
Tel: 972-980-5840
fax: 972-980-5841

Amendment — Serial No. 09/847,503..Page 14